

1

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 986 209 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

15.03.2000 Bulletin 2000/11

(51) Int. Cl.⁷: H04L 9/32

(21) Application number: 99112066.8

(22) Date of filing: 22.06.1999

(84) Designated Contracting States:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE

Designated Extension States:

AL LT LV MK RO SI

(30) Priority: 11.09.1998 JP 25781398

(71) Applicant:

MITSUBISHI DENKI KABUSHIKI KAISHA
Tokyo 100-8310 (JP)

(72) Inventors:

- Nakamura, Hiroshi,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)

- Fujii, Teruko,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)
- Sadakane, Tetsuo,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)
- Baba, Yoshimasa,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)

(74) Representative:

Pfenning, Meinig & Partner
Mozartstrasse 17
80336 München (DE)

(54) Remote authentication system

(57) To obtain a remote authentication system that securely authenticates with protecting biometrics information, which is user's personal information, and is firm on security when performing authentication of a person with the biometrics information, and a remote authentication method. The present invention encrypts biometrics information that is user's personal information, and transfers the biometrics information over a network in such a state that only an authentication server, which the user assigns, can decode the biometrics information. Therefore, it is possible to securely protect user's privacy that is the biometrics information in a style of reflecting user's intention, and to prevent reuse of invalid authentication information since it is possible to confirm the date and time, when the authentication information was generated, by the authentication server. Furthermore, it is possible to keep the security of a system firm since an authenticated side can confirm whether the user is authenticated.

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to a remote authentication system identifying a person with biometrics.

2. Description of the Related Art

[0002] Heretofore, so as to perform security protection in an information processing system connected to a network, it is necessary to identify a person and to judge approval or disapproval of access of the person, that is, to perform authentication. In addition, in cash dispensers of banks and the like, authentication for identifying a person and accessing the person's transaction information, and authentication for entrance into and exit from confidential research sites, membership clubs, and the like, which have high confidentiality, are performed.

[0003] Identification of a person and authorization of the person's qualification, that is, authentication is performed with a magnetic card, an IC card, which are positioned similarly to an identification card and the like, and the person's memory such as a password, and combination of them. There are problems that the authentication cannot be performed because the password is forgotten, and the magnetic card and IC card are lost or broken, and another person, who is not the principal, is authenticated with masquerading by burglary and leakage of password information.

[0004] In addition, as one of means for authenticating a user over a network, there is a digital signature for indirectly authenticating the user by authenticating a message created by the user. In the digital signature, first, a message sender attaches a cryptogram that is encrypted from a message digest, into which an original message is compressed, with the sender's cryptographic key to the message. A message receiver confirms that the message is one, which the sender himself/herself sent, and that the message is not tampered, by creating a message digest from the message received, decoding the message digest from the cryptogram, which is attached, with the sender's decoding key, and confirming coincidence of these two message digests.

[0005] In addition, in the above-described encryption method, there are a common key encryption method, using the same key for a cryptographic key and a decoding key, and a public key encryption method using different keys for the cryptographic key and decoding key. In the public key encryption method, when one key is set as a secret key and is kept safely and another key is officially announced as a public key, the cryptogram encrypted with the public key cannot be decoded into the original message if a receiver has not the secret key,

and hence the sender can transfer the message in such a form that only the receiver, who is desired by the sender, can decode, and the cryptogram encrypted with the secret key can be decoded with the public key into the original message, and hence the receiver can authenticates that the message is one from the sender herself/himself having the secret key.

[0006] Heretofore, although, in RFC1421 and RFC1422 (PEM: Privacy Enhancement for Internet Electronic Mail) that are registered in RFC (Request For Comment) of IETF (Internet Engineering Task Force), the digital signature and message encryption are performed with the public key encryption method and common key encryption method, there is a problem that it is necessary to administrate the secret key on the sender's hands since the sender uses the own secret key, for example, to safely keep the secret key with saving the secret key in a floppy disk, a magnetic card, and an IC card.

[0007] On the other hand, in the authentication with biometrics information, which is a person's biological characteristic such as finger print information, palm print information, handwriting information, and retina information, it is difficult to perform masquerade and is unnecessary to administrate the information of the secret key so long as the user himself/herself presents, and it is possible to resolve the complexity of keeping a baggage and the threat of loss at the time of the authentication of a person and the complexity of memory at the time of the authentication of a password with the magnetic card and IC card. Nevertheless, there are problems that, if the authentication with the biometrics information is necessary in a wide range, the equipment for performing the centralized administration and authentication of the biometrics information is necessary, and that it is necessary to keep security with concealing the user's biometrics information at the time of transferring the biometrics information to the equipment, performing the authentication, from the viewpoint of protection of privacy.

[0008] Furthermore, in general, random numbers are for creating a cryptographic key in a system creating the cryptographic key used for concealing the biometrics information. Nevertheless, there is also a problem that it is important to eliminate the tendency of the random numbers so as to make it difficult to break the cryptographic key.

[0009] In addition, an apparatus acquiring biometrics should be properly administrated from the viewpoint of protection of users' privacy, and it is necessary to authenticate an administrator. Nevertheless, there is a problem that, since another person cannot act for the administrator if the authentication of this administrator was performed with biometrics, another person can never perform the access to the biometrics acquisition apparatus including initialization. Furthermore, there is a problem that even a valid administrator can never perform the access to the biometrics acquisition apparatus

including initialization, if the biometrics used for the authentication is largely changed or lost by suffering damage in an accident in case of the valid administrator.

[0010] Moreover, in general, a system performing user authentication is required to early find an invalid authentication, for example, as for a cash card in a bank, there is means for making a cash card unusable if authentication with a preset number of times of password inputs is unsuccessful. Also, a user authentication system with the biometrics is required to early find an invalid authentication. Nevertheless, a condition of biometrics is different every person, for example, in a system authenticating a person with finger print matching, a minimum matching rate identifying a person as the principal is determined, but a person whose finger is rough or worn gets a low matching rate even if the person can obtain the best biometrics information at that time, and a failure probability of the authentication itself increase if the matching rate decreases due to a minor failure such as insufficient contact at the time of acquiring the finger print. Therefore, there is a problem that it cannot be equally performed for all the persons that it is judged to be an unsuccessful authentication within only the preset number of times.

SUMMARY OF THE INVENTION

[0011] The present invention is to solve above problems, and an object of the present invention is to provide a remote authentication system which securely authenticates with protecting biometrics information, which is user's personal information, and is firm on security when performing authentication of a person with the biometrics information, and a remote authentication method.

[0012] In a remote authentication system, in which an authentication server, an application server, and a user terminal are connected to a network respectively, and which authenticates a user using the user terminal, a remote authentication system according to a first invention is a system, wherein the authentication server has a pair of a public key and a secret key in a public key encryption method, announces the public key, and conceals the secret key, wherein at least one kind or a plural kind of biometrics acquisition apparatus is connected to the user terminal; wherein the biometrics acquisition apparatus: encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key; acquires the public key of the authentication server, which the user assigns; and encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest

encrypted with connecting the date and time information with the common key, as authentication information to the user terminal; and wherein the user terminal and application server transfer the authentication information to the authentication server, and the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; and encrypts result of authentication and a message digest of the result of the authentication with the secret key and transfers both to the application server.

[0013] In addition, in a remote authentication system, in which an authentication server and a user terminal are connected to a network respectively, and which authenticates a user using the user terminal, a remote authentication system according to a second invention is a system, wherein the authentication server has a pair of a public key and a secret key in a public key encryption method, announces the public key, and conceals the secret key; wherein at least one kind or a plural kind of biometrics acquisition apparatus is connected to the user terminal; wherein the biometrics acquisition apparatus: encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, further encrypts the message digest with the common key; acquires the public key of the authentication server, which the user assigns, and encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal; wherein the user terminal transfers the authentication information to the authentication server; and wherein the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; and encrypts result of authentication and a message digest of the result of the authentication and transfers both to the user terminal.

[0014] In addition, a remote authentication system is a system, wherein a biometrics acquisition apparatus: transfers biometrics information to a user terminal without encrypting the biometrics information at the time of authentication; encrypts the user's biometrics information, which the user terminal obtains, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, encrypts the message digest with the common key; acquires a public key of an authentication server,

which the user assigns; encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information.

[0015] Furthermore, a remote authentication system according to a fourth invention uses biometrics information as a part or all of random numbers for creating a common key in a common key encryption method for encrypting the user's biometrics information acquired, at the time of authentication.

[0016] A remote authentication system according to a fifth invention is a system, wherein a biometrics acquisition apparatus includes; an authentication unit of an administrator administrating the biometrics acquisition apparatus; and an authentication unit of an initializer initializing the biometrics acquisition apparatus, wherein the two authentication units perform authentication separately, and can perform only the initialization with authentication of the initializer.

[0017] A remote authentication system according to a sixth invention is a system, wherein an authentication server saves historic records of matching rates that are results of matching biometrics at the time of user authentication; compares a matching rate with an average matching rate at the time of identifying a user as a principal until the previous occasion if the authentication server does not identify the user as the principal at the time of user authentication; confirms whether the matching rate at this time changes more largely than a preset value determined by an administrator; and informs a contact, who is registered beforehand, if a number of failed times due to changes more largely than the fixed value reaches a fixed value determined by the administrator.

[0018] A remote authentication system according to a seventh invention is a system, wherein an authentication server saves historic records of matching rates that are results of matching biometrics at the time of user authentication; compares a matching rate with a matching rate at the time of identifying a user as a principal until the previous occasion at the time of user authentication if the authentication server identifies the user as the principal; makes the user authentication unsuccessful if the two matching rates are the same rates and a message digest of biometrics information is not saved, performs message digest calculation of biometrics information at this time, saves the message digest of biometrics information with the matching rate; saves a message digest of biometrics information at this time with a matching rate as a pair with calculating the message digest of biometrics information at this time if the two matching rates are the same and a message digest is saved, compares the message digest of biometrics information at this time with the message digest of biometrics information at the same matching rate in the

past, identifies the user as a principal if both message digests are different from each other; does not identify the user as a principal if a pair of a matching rate and a message digest at this time completely coincides with a pair of a matching rate and a message digest in the past; and informs a contact, who is registered beforehand, if a number of cases that the pair of the matching rate and message digest at this time completely coincides with the pair of the matching rate and message digest in the past reaches a value equal to or larger than a fixed value which is determined by an administrator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019]

Fig. 1 is a block diagram showing the configuration of a first embodiment of an Web system where a remote authentication system according to the present invention is applied;

Fig. 2 is a timing chart for explaining the processing of authentication in the Web system in Fig. 1;

Fig. 3 is a block diagram showing the configuration of a second embodiment of a database retrieval system where a remote authentication system according to the present invention is applied;

Fig. 4 is a timing chart for explaining the processing of authentication in the database retrieval system in Fig. 3;

Fig. 5 is a block diagram showing the configuration of a third embodiment of an Web system where a remote authentication system according to the present invention is applied;

Fig. 6 is a timing chart for explaining the processing of authentication in the Web system in Fig. 5;

Fig. 7 is a block diagram showing the configuration of a fourth embodiment at the time of administration of a finger print acquisition apparatus where a remote authentication system according to the present invention is applied;

Fig. 8 is a block diagram showing the configuration of a fifth embodiment of an authentication server where a remote authentication system according to the present invention is applied.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Hereinafter, embodiments of the present invention will be described with reference to drawings.

Embodiment.1

[0021] Fig. 1 shows the configuration of a Web system 1 where the present invention is applied. Over a network 2, an authentication server 3, an Web server 4 that is an application server, and a user terminal 5 are connected, and a biometrics acquisition apparatus 6 is connected to the user terminal 5. In this Web system 1, if a user

accesses the Web server 4 through the user terminal 5, the Web server 4 receives user's personal authentication from the authentication server 3, and according to the result, the Web server 4 performs access control to the user.

[0022] The authentication server 3 is a computer system (hereinafter, this is shown as a system having a CPU, memory, a disk, communication control, and the like) such as a personal computer and a workstation that are composed of an authentication controller 3A, an encryption processing unit 3C, and an authentication information database 3B, and announces one key in a public key method as a public key and conceals another key as a secret key.

[0023] In addition, the Web server 4 is a computer system such as a personal computer and a workstation where a Web server database 4A, an encryption processing unit 4D, an authentication request unit 4B, and an application of a Web server software 4C (hereinafter, software is written as S/W) that is an application requiring personal authentication operate.

[0024] In addition, the user terminal 5 is a computer system such as a personal computer and a workstation where a browser 5A displaying information of the Web server terminal 4, and authentication information acquisition S/W 5B operate. Furthermore, a biometrics acquisition apparatus 6 is connected to the user terminal 5. The biometrics acquisition apparatus 6 represents a finger print acquisition apparatus 7 and a palm print acquisition apparatus 8 that acquire finger print of a human body and palm print information with image processing as biometrics information, a character recognition tablet 9 acquiring handwriting information, which a user draws, as biometrics information, a retina acquisition apparatus 10 acquiring retina information of a human body as the biometrics information with eyeground (fundus) scanning and the like, and the like.

[0025] Here, a case that the finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be described as an example. In addition, the biometrics information acquired by the biometrics acquisition apparatus 6 such as the finger print acquisition apparatus 7 can be image data, image data that is not processed such as electrostatic data, and characteristics of point data obtained by extracting characteristics from image data. The finger print acquisition apparatus 7 is composed of a finger print information acquisition unit 7A acquiring finger print information with image processing and the like and transferring the finger print information to the user terminal, an encryption processing unit 7B encrypting the finger print information, and a public key acquisition unit 7C acquiring a public key of the authentication server 3.

[0026] Next, operation will be described.

[0027] A flow of authentication processing in the Web system 1 like this is shown in Fig. 2.

[0028] First, a case (SP5) that a user accesses information in the Web server database 4A, which has high

confidentiality, in the Web server 4 with the browser 5A that is an application operating in the user terminal 5 will be described. The Web server S/W 4C, which is an application performing access control of the information having high confidentiality, is required to perform the user authentication so as to judge whether the user has an access authority.

[0029] The authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information, which is biometrics information necessary for the authentication, from the finger print acquisition apparatus 7 (SP6). At this time, the S/W 4C may operate with cooperating with other S/W (software such as a driver acquiring the authentication information).

[0030] The finger print information acquisition unit 7A in the finger print acquisition apparatus 7, which is instructed to acquire the finger print information by the authentication information acquisition S/W 5B in the user terminal 5, acquires the finger print information from the user (SP1). Although the encryption processing unit 7B encrypts this finger print information since this finger print information is user's inherent personal information, first, the encryption processing unit 7B creates a common key in the common key method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 7B acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0031] The public key acquisition unit 7C in the finger print acquisition apparatus 7 acquires a public key of the authentication server from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry. Alternatively, if the finger print acquisition apparatus 7 is properly administrated, the public key of the authentication server 3 is fixedly saved in the public key acquisition unit 7C in the finger print acquisition apparatus 7, and hence the user may use the public key after recognizing the public key. Next, the encryption processing unit 7B encrypts the common key with the public key of the authentication server 3 (SP3).

[0032] Then, the finger print acquisition unit 7A transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key as the authentication information to the authentication information acquisition S/W 5B in the user terminal 5 (SP4).

[0033] The authentication information acquisition S/W 5B in the user terminal 5 transfers the authentication information, which is acquired, to the Web server 4 through the browser 5A. At this time, the browser 5A transfers the authentication information with adding a user ID such as a user name and a mail address, which the browser 5A acquires separately (SP7).

[0034] The authentication request unit 4B in the Web

server 4 transfers the authentication information, which the authentication request unit 4B acquires through the Web server S/W 4C, to the authentication controller 3A in the authentication server 3 (SP9).

[0035] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which are transferred, in the authentication server 3 with the message digest decoded from the message digest created with connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0036] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. This result of the authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 4B in the Web server 4 of the result of the authentication with including the message digest, which is encrypted, in the result of the authentication (SP13).

[0037] The authentication request unit 4B in the Web server 4 that receiving the result of the authentication informs the encryption processing unit 4D of the result of the authentication. The encryption processing unit 4D decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 4B is informed from the encryption processing unit 4D that the encryption processing unit 4D confirmed that the information was the valid information from the authentication server 3, the authentication request unit 4B informs the Web server S/W 4C of the result of the authentication. The Web server S/W 4C judges approval or disapproval of

access to the information in the Web server database, which has high confidentiality, to the user according to the result of the authentication (SP11). For example, the Web server S/W 4C performs operation to the user access such as the display of the confidential information.

[0038] In this manner, the finger print information that is user's personal information is encrypted with the common key created, the common key is encrypted with the public key of the authentication server 3, which the user set, and the public key of the authentication server 3 is directly set by the user in the finger print acquisition apparatus 7. Hence, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server 3, which the user assigned, can decode the finger print information. Furthermore, a user can instruct only a public key of the authentication server 3 with a floppy disk, a magnetic card, an IC card, or key entry to the finger print acquisition apparatus 7, there is no problem on security even if the floppy disk, magnetic card, or IC card is lost or stolen, which saves this public key, and the user can receive the personal authentication with a substitute, which saves the same public key or the same article. There is another effect that it is unnecessary to perform processing such as special notification and reissue at the time of loss and burglar and it is possible to lighten the administration load.

[0039] In addition, since the data and time, when the authentication information was created, is confirmed in the authentication server 3, it is possible to prevent reuse of the invalid authentication information, and to keep security high since it can be confirmed in the Web server 4 in the authentication requester's side whether the authentication is performed by the authentication information authentication server 3.

[0040] Although the present invention is applied in the Web system 1 in this embodiment, the same effect can be obtained even if the Web server S/W 4C and browser 5A are other applications, constructing another system, such as accounting information administration server S/W and accounting information administration client S/W, and database retrieval server S/W and database retrieval client S/W.

Embodiment 2

[0041] This embodiment is obtained by simplifying the first embodiment, and the Web server 4 and user terminal 5 in Fig. 1 become only a user terminals 5 in Fig. 3. Since, in Fig. 3 where the same symbols are assigned to the parts corresponding to the parts in Fig. 1, applications for which the personal authentication is necessary are present in only the user terminal 5, the Web server S/W 4C and two applications, constructing the browser 5A,

that are shown in Fig. 1 are replaced to database retrieval S/W 5E, and the Web server database 4A is replaced to a local database 5C. In this case, the authentication request unit 4B and encryption processing unit 4D that construct the Web server 4 in Fig. 1 become a component of the user terminal 5 in Fig. 3.

[0042] In the second embodiment, the user terminal 5 is a computer system such as a personal computer and a workstation, where the local database 5C, an encryption processing unit 5F, a authentication request unit 5D, a database retrieval S/W 5E that is an application for which the personal authentication is required, and authentication information acquisition S/W 5B operate. In addition, a biometrics acquisition apparatus 6 is connected to the user terminal 5, and has the same configuration as that in the first embodiment. Furthermore, the authentication server 3 also has the same configuration as that in the first embodiment described above.

[0043] Here, a case that a finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be exemplified.

[0044] Next, operation will be described.

[0045] Fundamentally, this is similar to that in the first embodiment, and in Fig. 4 where the same symbols are assigned to the parts corresponding to those in Fig. 2, first, a case that a user accesses information in the local database 5C, which has high confidentiality, with the database retrieval S/W 5E that is an application operating in the user terminal 5 will be described. The database retrieval S/W 5E that is an application performing access control of the information having high confidentiality is required to perform the user authentication so as to judge whether the user has access authorization (SP5).

[0046] The authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information, which is necessary for the authentication, from the finger print information acquisition apparatus 7 (SP6). At this time, this S/W 5B may cooperate with other S/W (software such as a driver acquiring the authentication information).

[0047] The authentication information acquisition unit 7A in the finger print acquisition apparatus, which is instructed to acquire the finger print information from the authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information from the user (SP1). Although encryption processing unit 7B encrypts this finger print information since this finger print information is user's personal information, first, the encryption processing unit 7B creates a common key in the common key encryption method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 7B acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0048] The public key acquisition unit 7C in the finger print acquisition apparatus 7 acquires the public key of the authentication server 3 from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry. Alternatively, if the finger print acquisition apparatus 7 is properly administrated, the public key of the authentication server 3 is fixedly saved in the public key acquisition unit 7C in the finger print acquisition apparatus 7, and hence the user may use the public key after recognizing the public key. Next, the encryption processing unit 7B encrypts the common key with the public key of the authentication server 3 (SP3). Then, the finger print acquisition unit 7A transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key as the authentication information to the authentication information acquisition S/W 5B in the user terminal 5 (SP4).

[0049] The authentication information acquisition S/W 5B in the user terminal 5 acquires a user ID such as a user name and a mail and adds them to the authentication information (SP7).

[0050] The authentication request unit 5D transfers this authentication information to the authentication controller 3A in the authentication server 3 (SP7).

[0051] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which is transferred, in the authentication server 3 with the message digest decoded from the message digest obtained by connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0052] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. This result of the authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is

encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 5D in the user terminal 5 of the result of the authentication with including the message digest, which is encrypted, in the result of the authentication (SP13).

[0053] The authentication request unit 5D in the user terminal 5 that receiving the result of the authentication informs the encryption processing unit 5F of the result of the authentication. The encryption processing unit 5F decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 5D receives from the encryption processing unit 5D the result of confirmation that the information is the valid information from the authentication server 3, the authentication request unit 5D informs the database retrieval S/W 5E of the result of the authentication. The database retrieval S/W 5E judges approval or disapproval of access to the information in the local database 5C, which has high confidentiality, to the user according to the result of the authentication. For example, the database retrieval S/W 5E performs operation to, the user access such as the display of the confidential information (SP11).

[0054] According to this configuration, when the user terminal 5 requests the authentication server 3 to perform the personal authentication, it is possible to obtain the same effects as those in the first embodiment.

[0055] Although the present invention is applied in the database retrieval system 1 in this embodiment, the same effects can be obtained even if the database retrieval S/W is an application, constructing another system, such as accounting information administration S/W.

Embodiment 3.

[0056] This third embodiment is an embodiment where the encryption processing unit 7B and public key acquisition unit 7C in the finger print acquisition apparatus 7 that is a biometrics acquisition apparatus 6 in the first embodiment present in the user terminal 5.

[0057] In Fig. 5 where the same symbols are assigned to the parts corresponding to those in Fig. 1, the user terminal 5 is a computer system such as a personal computer and a workstation, where a browser 5A displaying the information of the Web server terminal 4, an encryption processing unit 5F encrypting the finger print information, a public key acquisition unit 5G acquiring the public key of the authentication server 3, and an authentication information acquisition S/W 5B operate. In addition, a biometrics acquisition apparatus 6 is connected to the user terminal 5. Furthermore, the authentication server 3 and Web server 4 have the same

configuration as that in the first embodiment.

[0058] In addition, the biometrics information which the biometrics acquisition apparatus 6 in this embodiment acquires can be image data, image data that is not processed such as electrostatic data, and also characteristic point data obtained by extracting characteristics from image data. The biometrics acquisition apparatus 6 can be a simple device that only acquires image data and does not have a CPU. Here, a case that the finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be exemplified.

[0059] The finger print acquisition apparatus 7 is composed of a finger print information acquisition unit 7A that acquires the finger print information by performing image processing and the like and transfers the finger print information to the user terminal.

[0060] Next, operation will be described.

[0061] Fundamentally, the operation is the same as that in the first embodiment, in Fig. 6 where the same symbols are assigned to the parts corresponding to those in Fig. 2, first, a case that a user accesses the information in the Web server database 4A, which has high confidentiality, in the Web server 4 with the browser 5A that is an application operating in the user terminal 5 will be described (SP5). The Web server S/W 4C, which is an application performing access control of the information having high confidentiality, is required to perform the user authentication so as to judge whether the user has an access authority.

[0062] The authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information, which is biometrics information necessary for the authentication, from the finger print acquisition apparatus 7 (SP6). At this time, the S/W 4C may operate with cooperating with other S/W (software such as a driver acquiring the authentication information).

[0063] The finger print information acquisition unit 7A in the finger print acquisition apparatus 7 which is instructed to acquire the finger print information by the authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information from the user (SP1), and transfers the finger print information to the authentication information acquisition S/W 5B in the user terminal 5 (SP4).

[0064] The authentication information acquisition S/W 5B in the user terminal 5 makes the encryption processing unit 5F encrypt this finger print information since this finger print information is user's inherent personal information. First, the encryption processing unit 5F creates a common key in the common key method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 5F acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0065] The public key acquisition unit 5G in the user

terminal 5 acquires a public key of the authentication server from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry.

[0066] Next, the encryption processing unit 5F encrypts the common key with the public key of the authentication server 3 (SP3). Then, the authentication information acquisition S/W 5B transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key, the acquired authentication information as the authentication information to the Web server 4 through the browser 5A. At this time, the browser 5A transfers the authentication information with adding a user ID such as a user name and a mail address, which the browser 5A acquires separately, to the authentication information (SP7).

[0067] The authentication request unit 4B in the Web server 4 transfers the authentication information, which the authentication request unit 4B acquires, to the authentication controller 3A in the authentication server 3 through the Web server S/W 4C (SP9).

[0068] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which are transferred, in the authentication server 3 with the message digest decoded from the message digest obtained by connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0069] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. The result of this authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 4B in the Web server 4 of the result of the authentication with including the message digest, which

is encrypted, in the result of the authentication (SP13).

[0070] The authentication request unit 4B in the Web server 4 receiving the result of the authentication informs the encryption processing unit 4D of the result of the authentication. The encryption processing unit 4D decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 4B is informed from the encryption processing unit 5D that it was confirmed that the information was the valid information from the authentication server 3, the authentication request unit 4B informs the Web server S/W 4C of the result of the authentication. The Web server S/W 4C judges approval or disapproval of access to the information in the Web server database 4A, which has high confidentiality, to the user according to the result of the authentication. For example, the Web server S/W 4C performs operation to the user access such as the display of the confidential information (SP11).

[0071] In this manner, the finger print information that is user's personal information is encrypted with the common key created, the common key is encrypted with the public key of the authentication server 3, which the user set, and the public key of the authentication server 3 is directly set by the user in the user terminal 5. Hence, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server 3, which the user assigned, can decode the finger print information. Nevertheless, although security becomes low in comparison with a case that the finger print information is encrypted from the finger print acquisition apparatus 7 since there arises a period, when the finger print information exists in the user terminal 5 without being encrypted, there is no problem if the user terminal 5 itself is properly administrated, and there is an effect that the configuration of the finger print acquisition apparatus 7 becomes simple since the encryption processing unit and public key acquisition unit are unnecessary in the finger print acquisition apparatus 7.

As effects except the above-described effects, the similar effects as those in the first embodiment can be obtained. In addition, this embodiment can be applied also to the application such as the database retrieval S/W 5E, which are shown in the second embodiment, and hence it is possible to obtain the same effects.

[0072] Furthermore, in all of the first, second, and third embodiments, a common key for encrypting the user's biometrics information obtained is created. Nevertheless, it is necessary to eliminate the tendency of the random numbers for creating the common key so as to

make it difficult to break the common key. Since the biometrics information generally has values different every acquisition, the message digest of the biometrics information acquired is used as a part or all of the random numbers.

[0073] As described above, it is simply performed to eliminate the tendency of the generated random numbers since the random numbers generated from the message digest of the biometrics information acquired are generated. Furthermore, since a part or all of this random numbers are used as the random numbers for generating the common key, it is possible to generate the random numbers irrelevant to the number of authentication times and the time and to construct a system that is strong on security against the decoding of the common key.

Embodiment 4.

[0074] Although only the valid administrator can perform the administration of the biometrics information acquisition apparatus, it is necessary that the administrator, being not authenticated, or another person acting for the administrator can perform initialization of a biometrics acquisition apparatus if there arises such a state that no one cannot authenticate the valid administrator. This case will be described with exemplifying such a case that, in the finger print acquisition apparatus in the first and second embodiments, the finger print acquisition apparatus is properly administrated and a public key of an authentication server is fixedly determined in the finger print acquisition apparatus.

[0075] Fig. 7 is the configuration at the time of administrating, that is, setting and changing the public key fixedly saved in a public key acquisition unit 12C in a finger print acquisition apparatus 12. An administration terminal 11 is a computer system such as a personal computer and a workstation, where an administration S/W 11A operates. The finger print acquisition apparatus 12 is composed of a finger print information acquisition unit 12A and an encryption processing unit 12B, a public key acquisition unit 12C, and an administration unit 12D.

[0076] The administration S/W 11A in the administration terminal 11 issues authentication request of an administrator to the finger print acquisition apparatus 12 so as to execute setting of the public key. Although an administrator authentication unit 12D1 in an administration unit 12D in the finger print acquisition apparatus 12 acquires administrator's finger print from the finger print information acquisition unit 7A and performs finger print matching of the administrator, the administrator authentication unit 12D1 may become in such a condition that the unit 12D1 cannot identify the administrator as the valid administrator. This corresponds to a case that the finger print itself is lost due to an injury of the administrator. In this case, although the administration S/W 11A instructs an initializer authentication unit 12D2 in the administration unit 12D in the finger print acquisition

apparatus 12 to perform initialization; the S/W 11A performs the authentication of the initializer with means, being set beforehand, such as a password. The initializer authentication unit 12D2 performs only the authentication of the initializer, only the initialization of the finger print acquisition apparatus is executed by the authentication of the initializer authentication unit 12D2.

[0077] In this manner, by providing the authentication means for an initializer separately from an ordinary administrator, there are such effects that it is possible to perform only the initialization if an administrator cannot be authenticated and suddenly becomes absent, and furthermore to prevent a person not having the initialization authority from invalidly performing the initialization.

Embodiment 5.

[0078] Fig. 8 shows an authentication server where means for finding invalid authentication is applied to the above-described authentication server so as to enhance reliability. An authentication server 13 is a computer system such as a personal computer and a workstation, which is composed of a logging unit 13D, an authentication controller 13A, an encryption processing unit 13C, and an authentication information database 13B.

[0079] The logging unit 13D in the authentication server 13 logs a matching rate that is the result of matching biometrics at the time of the user authentication. In addition, the logging unit 13D confirm that a matching rate at this time does not change more than or equal to a preset value determined by the administrator by comparing the matching rate at this time with the average matching rate at the time of identifying a user as the principal until the previous occasion if the authentication controller 13A does not identifies the user as the principal at the time of the user authentication. If the matching rate changes more than or equal to a fixed value, the logging unit 13D increases the number of failure times. If the number of failure times reaches the value more than or equal to a fixed value determined by the administrator, the logging unit 13D informs the administrator, who is registered beforehand, and the user herself/himself of the failure.

[0080] Since this structure informs the administrator and the user, who is personated, of the abnormal result of the matching that is unique in biometrics authentication, it is possible to early find the invalid authentication and to keep the high security of the system.

[0081] In addition, since biometrics information becomes information different every acquisition even if matching rates are the same, it is stochastically very small that biometrics information acquired in the past coincides with the new biometrics information. An invalidity-finding structure using this characteristic of the biometrics authentication will be described.

[0082] The logging unit 13D in the authentication server 13 that is shown in Fig. 8 compares a matching

rate at this time with the matching rate at the time of identifying a user as the principal until the previous occasion and confirms that both matching rates are the same if the authentication controller 13A identifies the user as the principal at the time of the user authentication. If the matching rates are the same and a message digest of the biometrics information is not saved, the logging unit 13D informs the authentication controller 13A of making the user authentication unsuccessful, and the authentication controller 13A makes the result of the authentication unsuccessful. At the same time, the logging unit 13D saves the message digest of the biometrics information with the matching rate. If the matching rates are the same and the message digest of the biometrics information is saved, the logging unit 13D calculates a message digest of the biometrics information at this time, compares this message digest with the message digest of the biometrics information at the same matching rate in the past. If both message digest are different from each other, the logging unit 13D identifies the user as the principal, but, if both coincide with each other, the logging unit 13D informs the authentication controller 13A of making the user authentication unsuccessful since there is a possibility of masquerade. The authentication controller 13A makes the result of the authentication unsuccessful. The logging unit 13D increases the number of failure times, at the same matching rate if the authentication is made unsuccessful due to coincidence of the matching rate and message digest, and, if this number of failure times reaches a value more than or equal to the fixed value determined by the administrator, the logging unit 13D informs the administrator and the user herself/himself that are registered beforehand.

[0083] Since this structure informs the administrator and the user, who is personated, of such an abnormal state that it is considered to be the masquerade caused by leakage of the biometrics information, it is possible to early find the invalid authentication and to keep the high security of the system. In addition, there are such effects that it is possible to reduce a storage area since the authentication server 3, an application server 4, an object which the logging unit 13D saves is the message digest of the biometrics information at the time of the second occasion, and a user terminal 5 are connected to a network 2 respectively, and which authenticates a user using the same matching rate after the second occasion, and wherein the user terminal, wherein the authentication server that it is possible to shorten the time consumed for comparison in comparison with the comparison, performed by using biometrics information itself, because of the secret key, and conceals the secret key, a comparison performed by using the message digests.

[0084] As described above, according to the present invention, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server, which the user assigned, can decode the finger print information, and it is possible to prevent invalid authentication information from being reused since the date

and time when the authentication information was created can be confirmed in the authentication server 3, and to keep the security of the system high since the authentication request side can confirm whether the user is authenticated by the authentication server.

[0085] Furthermore, although a user can instruct a public key of the authentication server, there is no problem on security even if the floppy disk, magnetic card, or IC card, which saves this public key, is lost or stolen, and the user can receive the personal authentication with a substitute, which saves the same public key or the same article. There is another effect that it is unnecessary to perform processing such as special notification and reissue at the time of loss and burglar and it is possible to lighten the administration load.

[0086] In addition, since the present invention creates random numbers, used for creating the common key, from the biometrics information acquired, it is possible to generate the random numbers irrelevant to the number of authentication times and the time, and to construct a system that is strong on security against the decoding of the common key.

[0087] Furthermore, by providing the authentication means for an initializer separately from an ordinary administrator, there are such effects that it is possible to perform the initialization even if an administrator suddenly becomes absent, and furthermore to prevent a person not having the initialization authority from invalidly performing the initialization.

[0088] Moreover, since the authentication server logs at the time of the user authentication and informs a person, who is registered beforehand, of the abnormal result of the matching that is unique in biometrics authentication, it is possible to early find the invalid authentication and to keep the high security of the system.

Claims

1. A remote authentication system in which an authentication server 3, an application server 4, an object which the logging unit 13D saves is the message digest of the biometrics information at the time of the second occasion, and a user terminal 5 are connected to a network 2 respectively, and which authenticates a user using the same matching rate after the second occasion, and wherein the authentication server 3 has a pair of a public key and a secret key in a public key encryption method, announces the public key by using biometrics information itself, because of the secret key, and conceals the secret key, a comparison performed by using the message digests.

2. The remote authentication system according to claim 1, wherein at least one kind or a plural kind of biometrics acquisition apparatus 6 is connected to the user terminal 5.

3. The remote authentication system according to claim 2, wherein the biometrics acquisition apparatus 6 encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information; creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key; acquires the public

key of the authentication server, which the user assigns, and encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal; 5
 wherein the user terminal and the application server transfer the authentication information to the authentication server; and
 wherein the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; encrypts result of authentication and a message digest of the result of the authentication; and transfers both to the application server. 10
 15
 20

2. A remote authentication system in which an authentication server 3, an application server 4, and a user terminal 5 are connected to a network 2 respectively, and which authenticates a user using the user terminal, wherein the authentication server has a pair of a public key and a secret key in a public key encryption method, announces the public key, and conceals the secret key, and at least one kind or a plural kind of biometrics acquisition apparatus 6 is connected to the user terminal; wherein the biometrics acquisition apparatus: encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, further encrypts the message digest with the common key; acquires the public key of the authentication server, which the user assigns; encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal; wherein the user terminal transfers the authentication information to the authentication server; and wherein the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; encrypts result of authentication and a message digest of the result of the authentication with the secret key; and transfers both to the user terminal. 25
 30
 35
 40
 45
 50
 55

3. The remote authentication system according to any one of claims 1 and 2, wherein the biometrics acquisition apparatus transfers biometrics information to the user terminal without encrypting the biometrics information at the time of authentication; and
 wherein the user terminal: encrypts the user's biometrics information, which is obtained, with a common key in a common key encryption method; acquires a public key of a authentication server that a user assigns; encrypts the common key with the public key of the authentication server; acquires date and time information, creates a message digest with connecting the date and time information with the common key, encrypts the message digest with the common key; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal. 60
 65
 70
 75
 80
 85

4. The remote authentication system according to any one of claims 1 to 3, wherein the user terminal uses biometrics information as a part or all of random numbers for creating the common key when, at the time of authentication, the user terminal creates the common key in a common key encryption method for encrypting the user's biometrics information acquired. 90
 95

5. The remote authentication system according to any one of claims 1 to 3; wherein the biometrics acquisition apparatus includes an authentication unit of an administrator administrating the biometrics acquisition apparatus and an authentication unit of an initializer initializing the biometrics acquisition apparatus; and
 wherein the two authentication units perform authentication separately, and performs initialization with authentication of the initializer even if the administrator is not authenticated. 100
 105
 110
 115
 120

6. The remote authentication system according to any one of claims 1 to 3, wherein the authentication server: saves a historic record of a matching rate that is result of matching biometrics at the time of user authentication; compares a matching rate with an average matching rate at the time of identifying a user as a principal until the previous occasion if the authentication server does not identify the user as the principal at the time of user authentication; confirms whether a matching rate at this time changes more largely than a preset value determined by an administrator; and informs a contact, who is registered beforehand, if a number of failed times due to changes more largely than a fixed value reaches a fixed value determined by the 125
 130
 135
 140
 145
 150

administrator, and performs message digest calculation of biometrics information at this time.

7. The remote authentication system according to any one of claims 1 to 3, wherein the authentication server saves historic records of matching rates that are results of matching biometrics at the time of user authentication; compares a matching rate with a matching rate at the time of identifying a user as a principal until the previous occasion at the time of user authentication if the authentication server identifies the user as the principal; makes the user authentication unsuccessful if the two matching rates are the same rates and a message digest of biometrics information is not saved, performs message digest calculation of biometrics information at this time, saves the message digest of biometrics information with the matching rate; saves a message digest of biometrics information at this time with a matching rate as a pair with calculating the message digest of biometrics information at this time if the two matching rates are the same and a message digest is saved, compares the message digest of biometrics information at this time with the message digest of biometrics information at the same matching rate in the past, identifies the user as a principal if both message digests are different from each other; does not identify the user as a principal if a pair of a matching rate and a message digest at this time completely coincides with a pair of a matching rate and a message digest in the past; and informs a contact, who is registered beforehand, if a number of cases that the pair of the matching rate and message digest at this time completely coincides with the pair of the matching rate and message digest in the past reaches a value equal to or more than a fixed value which is determined by an administrator.

40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9

FIG. 1

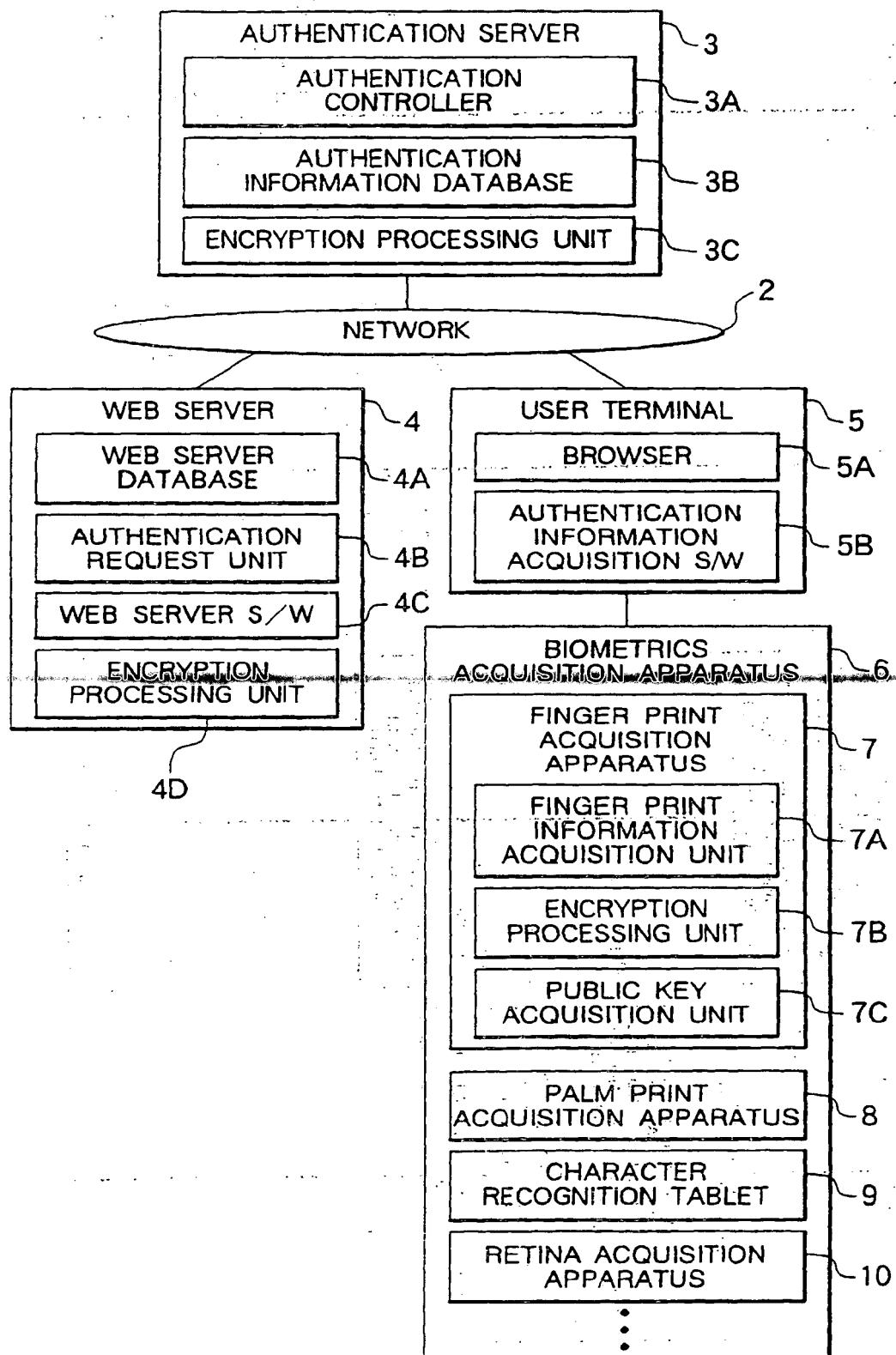


FIG. 2

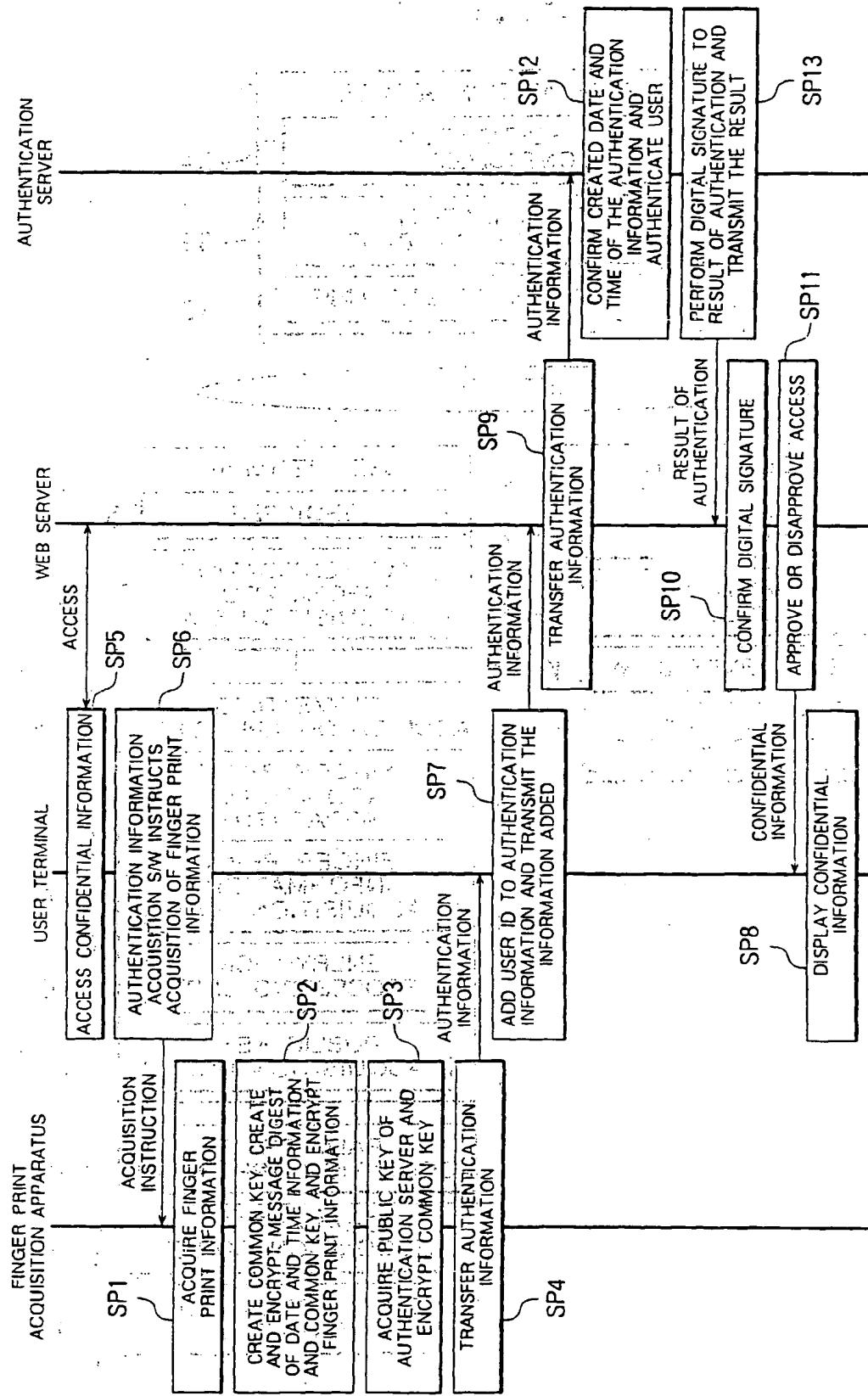


FIG. 3

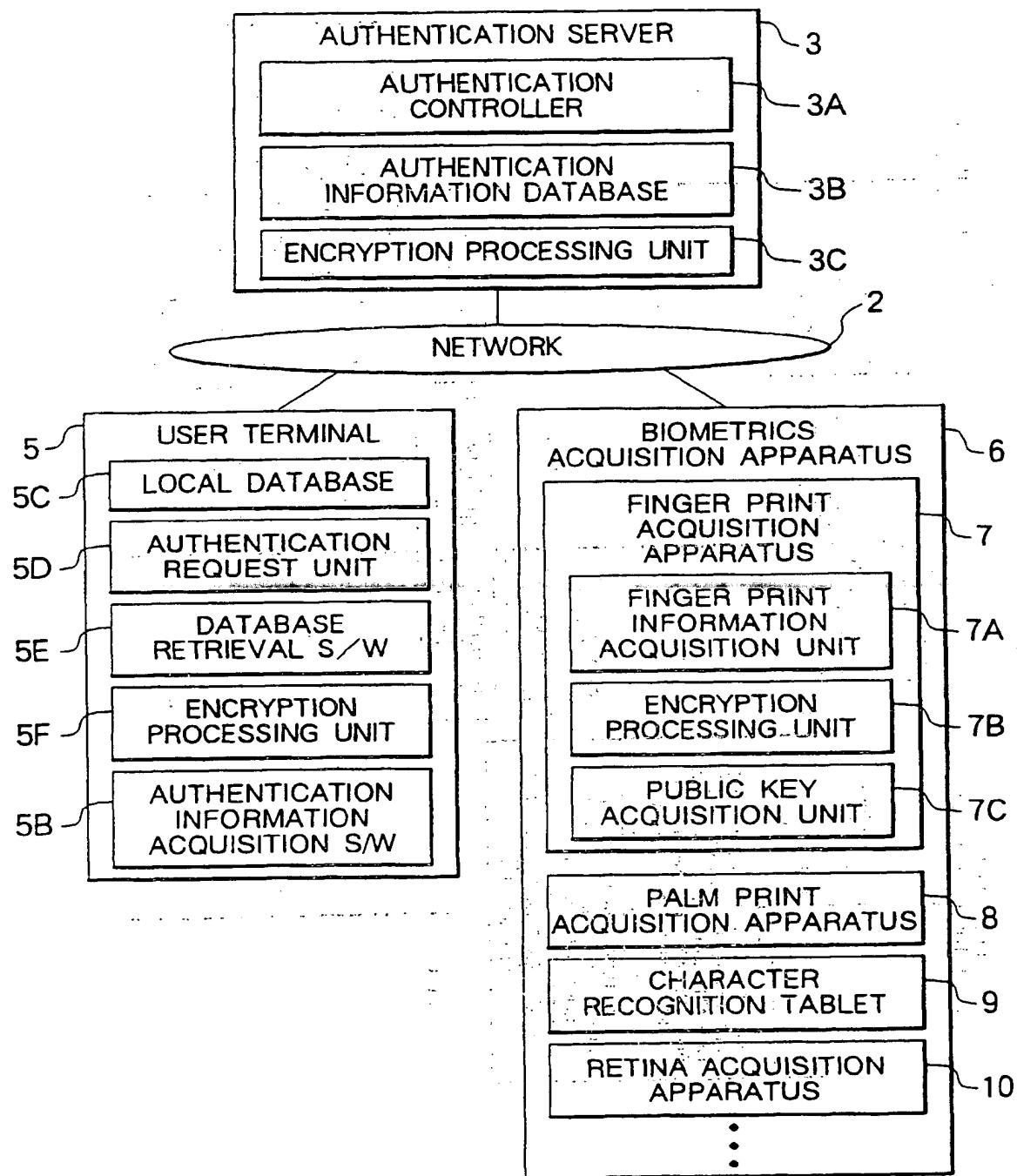


FIG. 4

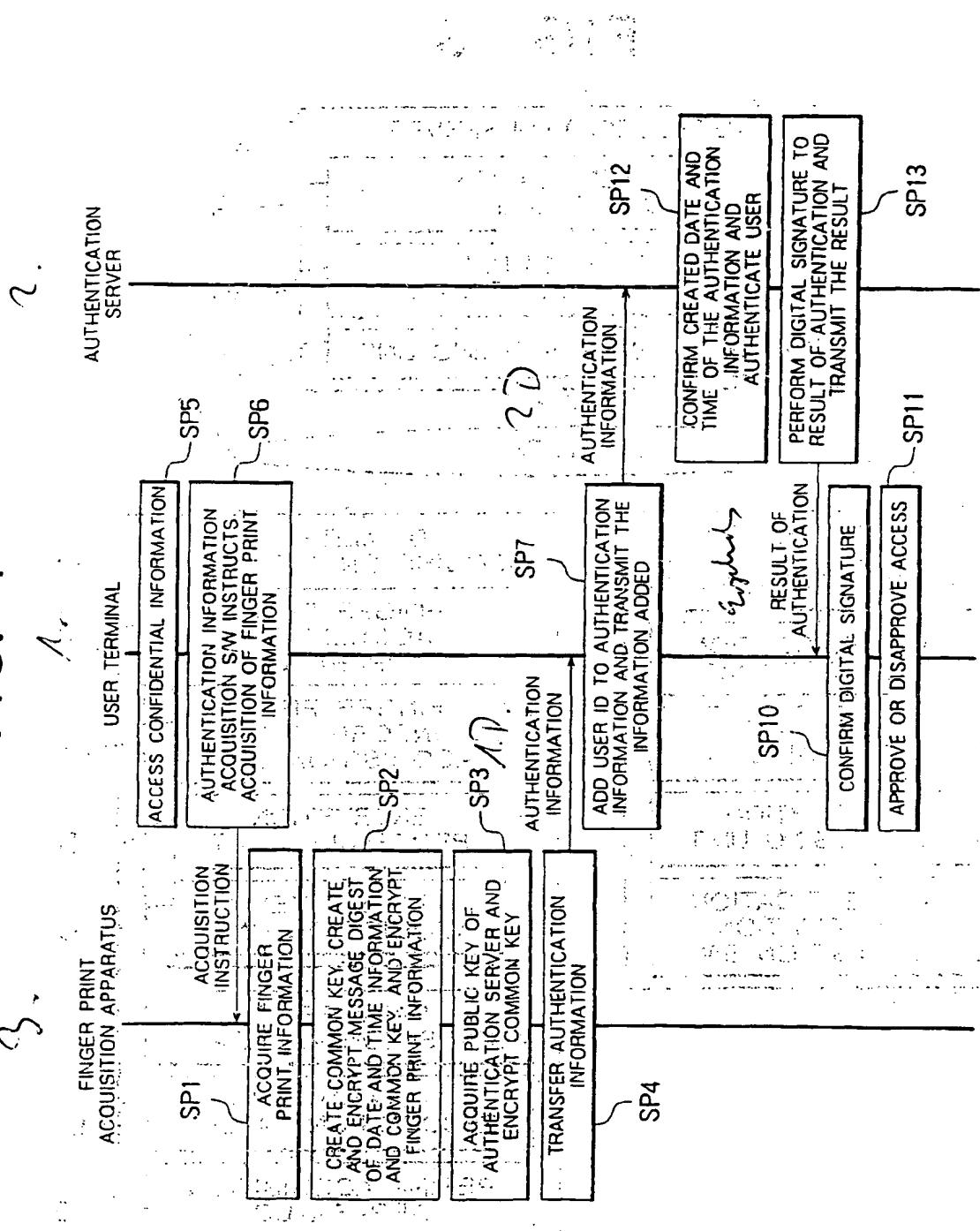


FIG. 5

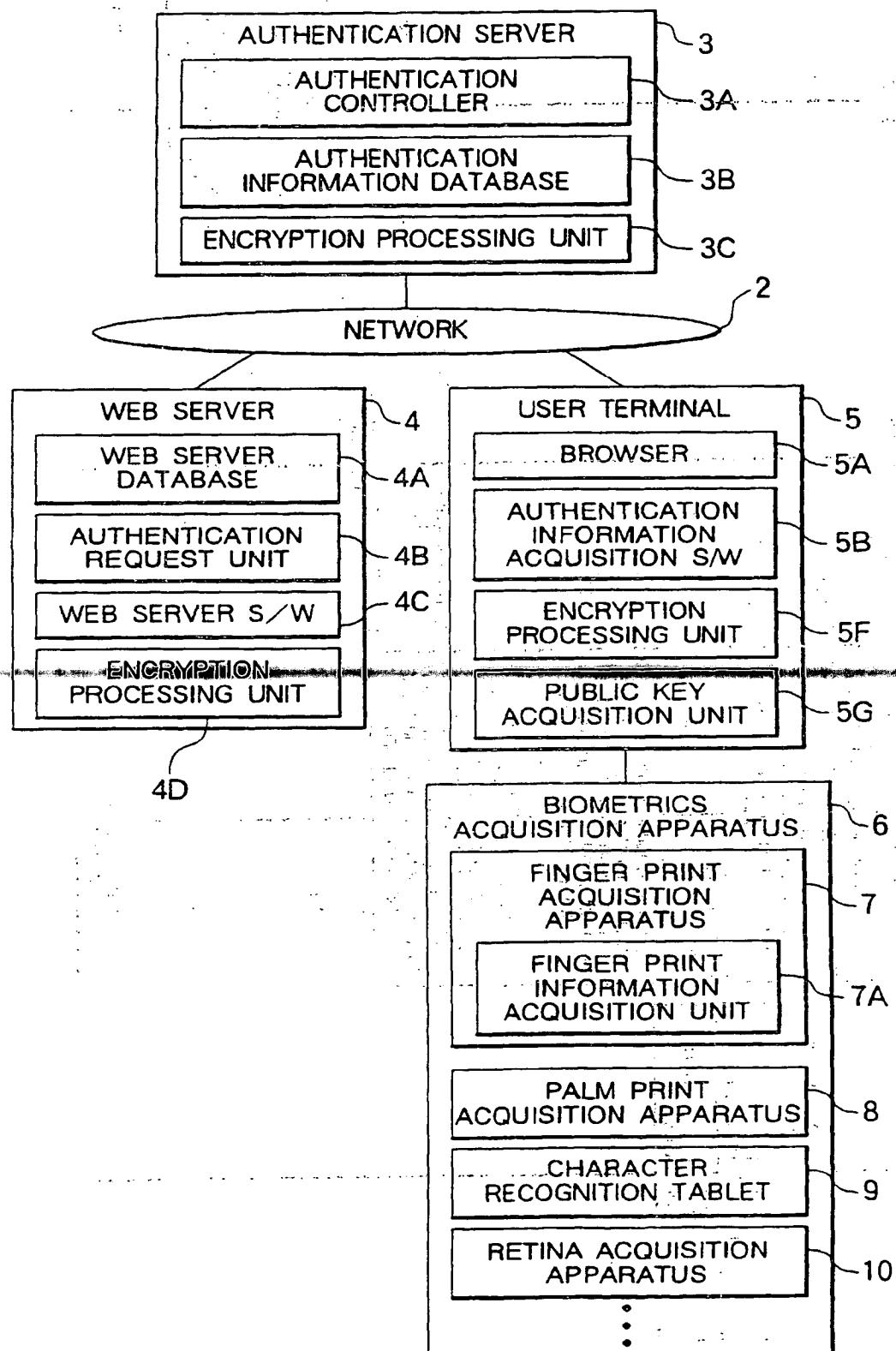


FIG. 6. *U. r.*

二

FINGER PRINT ACQUISITION APPARATUS

USER TERMINAL

111

5

וְרֵבֶת

SERVEN 1

AUTHENTICATION SERVER

WEB SERVER

TERMINAL

AUTHENTICATION SERVER

20

200

17

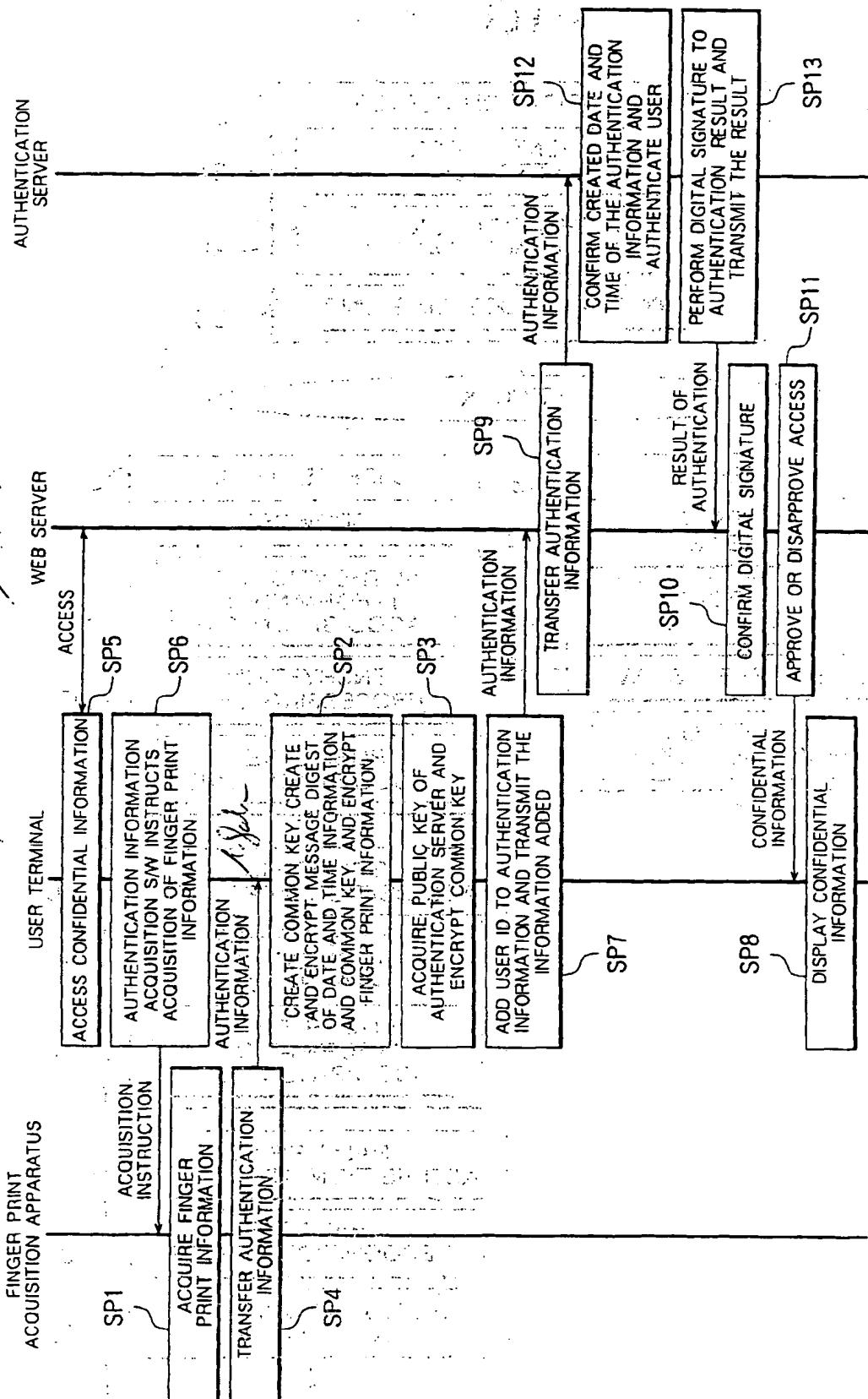


FIG. 7

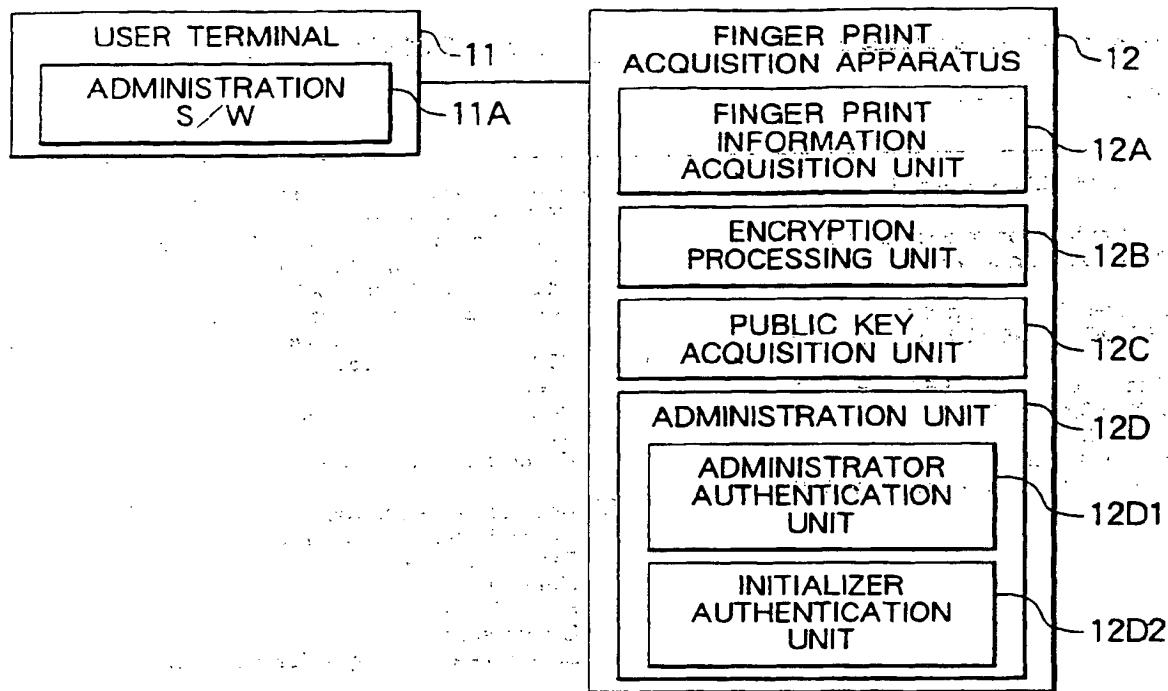


FIG. 8

